

## UNITED STATES DISTRICT COURT

for the  
Western District of ArkansasUS DISTRICT COURT  
WESTERN DISTRICT OF ARKANSAS  
FILED

JUN 04 2020

DOUGLAS F. YOUNG, Clerk  
By  
Deputy ClerkIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

The following account(s)

INFORMATION RELATED TO APPLE  
iCLOUD ACCOUNT(S), THAT IS STORED  
AT PREMISES CONTROLLED BY APPLE,  
INC. SEE ATTACHMENT A.

Case No.

5:20CM50

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A. This court has authority to issue this warrant under 18 U.S.C. §§ 2703(c)(1)(A) and 2711(3)(A) and Federal Rule of Criminal Procedure 41.

located in the Western District of Arkansas, there is now concealed (identify the person or describe the property to be seized):  
See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section  
18 U.S.C. 2522/2252A & 2251Offense Description  
Possession, Production & Transportation of Child  
Pornography

The application is based on these facts:

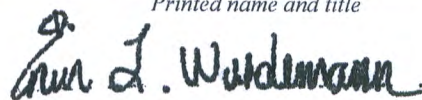
See Attached Affidavit of HSI Task Force Officer Thomas Wooten

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
Applicant's signature
HSI Task Force Officer, Thomas Wooten  
Printed name and title

Sworn to before me and signed in my presence.

Date: 6/4/2020

  
Judge's signature

City and state: Fayetteville, AR

Hon. Erin L. Wiedemann, U.S. Magistrate Judge

**ATTACHMENT C**

**UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF ARKANSAS**

**IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH Apple**  
iCloud accts: cocksuckerwithagun@gmail.com,  
pervyfwb@gmail.com, madwirelesspllc@gmail.com,  
fwb69@icloud.com, pervyfwb69@icloud.com,  
leatherneck4life@icloud.com, mattielawson@me.com  
THAT IS STORED AT PREMISES CONTROLLED  
BY APPLE, INC.

Case No. \_\_\_\_\_

**Filed Under Seal**

**Affidavit in Support of Application for Search Warrant**

I, Thomas Wooten, a Task Force Officer with Homeland Security Investigations (HSI),  
being duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information related to Apple iCloud accounts: cocksuckerwithagun@gmail.com, pervyfwb@gmail.com, madwirelesspllc@gmail.com, fwb69@icloud.com, pervyfwb69@icloud.com, leatherneck4life@icloud.com, mattielawson@me.com, as well as any and all account information associated with Matthew LAWSON that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple, Inc., to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the



information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Task Force Officer with the Department of Homeland Security, Homeland Security Investigations (“HSI”), currently assigned to the Assistant Special Agent in Charge Office in Fayetteville, Arkansas. Since June of 2000, I have been a police officer/detective with the Springdale, Arkansas Police Department. As such, I am authorized by the State of Arkansas to apply for and execute search warrants, arrest warrants and other instruments of the court. As a police officer/detective, I have received specialized training in matters related to criminal investigation, specifically but not limited to the area of sexual exploitation of minors, drug distribution, and money laundering. Since August of 2017, I have been assigned as a Task Force Officer to Homeland Security Investigations (HSI), a component of the U.S. Department of Homeland Security. As a Task Force Officer (TFO) with HSI, I primarily investigate crimes related to the sexual exploitation of minors. Prior to joining HSI, I attended a 40-hour training session covering Title 8, Title 18, Title 19 and Title 21 of the United States Code. As such, I am a law enforcement officer within the meaning of Section 115(c)(1) of Title 18 of the United States Code, who is authorized by law or Government agency to engage in or supervise the prevention, detection, investigation and/or prosecution of any violation of Federal and State criminal law. Since joining HSI as a Task Force Officer, your Affiant has received training in Cellebrite Mobile Forensics, Passmark Software/OSForensics Triage tools, and has obtained certifications as a Cellebrite Certified Operator, Cellebrite Certified Physical Analyst and OSForensics Triage Operator. This affidavit is being submitted based on information from my own investigative efforts as well as information obtained from others who have investigated this matter and/or have personal knowledge of the facts herein.

3. This Affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that evidence constituting violations of Title 18, United States Code, Sections 2251 (Production of Child Pornography) and 2252A(a)(5)(B) (Possession of Child Pornography) and 2252A(a)(1) and (b)(1) (Transportation of Child Pornography), are currently present on the item described as Attachment A.

5. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband/ fruits of these crimes further described in Attachment B.

6. On March 3, 2020, MATTHEW LAWSON was indicted by the Grand Jury in the Western District of Arkansas for the offenses of Transportation of Child Pornography (two counts) and Possession of Child Pornography (two counts). The investigation is ongoing.

#### **DEFINITIONS AND AUTHORITY**

7. This investigation concerns alleged violations of Title 18, United States Code, Section 2251 and 2252/2252A, specifically Production, Possession and Transportation of Child Pornography.

8. Under Title 18, United States Code, Section 2251, it is a federal crime for any person using any means or facility of interstate and foreign commerce, to entice, use, persuade ...a person that has not obtained the age of 18 years that will be caused to engage in sexually explicit conduct for the purpose of creating a visual depiction of such conduct. Under Title 18, United States Code, Section 2252/2252A, it is a federal crime for any person to knowingly



possesses child pornography as that term is defined by Title 18, United States Code, Section 2256. Under Title 18, United States Code, Section 2256(8)(A), it is a federal crime to knowingly transport and ship, using any means and facility of interstate commerce, visual depictions of child pornography.

9. The term “minor,” as used herein, is defined pursuant to Title 18, United States Code, Section 2256(1) as “any person under the age of eighteen years.”

### **PROBABLE CAUSE**

10. On September 05, 2019, Franklin County, Arkansas Deputies arrested MATTHEW LAWSON on state charges for Possession of a Controlled Substance (methamphetamine), Possession of Drug Paraphernalia, and Resisting Arrest. LAWSON was transported to the Franklin County Jail for incarceration and his vehicle was impounded to JLW Towing and Recovery, located in Ozark, Arkansas. LAWSON’S vehicle had a lien on it from the Auto Easy car lot, located in Springdale, Arkansas. The owners of Auto Easy were notified that the car was impounded, so they repossessed the vehicle to avoid any further impound fees. Auto Easy representatives towed the car back to Springdale, Arkansas and boxed up all of LAWSON’S personal belongings.

11. On September 12, 2019, Auto Easy employee, Demian Nacol, found a black Gigastone 32GB thumb drive connected to LAWSON’S car keys. Nacol plugged the thumb drive in to his work computer and discovered numerous images of child pornography. Subsequently Nacol called the Springdale Police Department to report the incident. Detective Hunter Helms (Badge# 376) responded to the Auto Easy car lot where he collected the evidence, obtained witness statements and filed a report.

12. On October 01, 2019, Detective Helms obtained a state search warrant to search the contents of the thumb drive which was signed and granted by Washington County Circuit Court Judge, John Threet. On October 03, 2019, your affiant received the thumb drive from Detective Helms and searched the digital storage device using Cellebrite UFED4PC and UFED Physical Analyzer. A physical extraction was obtained from the thumb drive and a Cellebrite UFED Physical Analyzer report was generated to review the contents of the digital storage drive. As a result of the physical extraction from the digital storage drive, approximately forty-three (43) videos of child pornography and two (2) picture files of child pornography were found stored on the 32GB thumb drive. Your Affiant also identified personal State of Arkansas tax documents belonging to LAWSON saved on the thumb drive.

13. Your Affiant viewed all of the digital images/videos and determined them to in fact be images and videos of child pornography. On October 11, 2019, your Affiant again viewed and described three of these files as follows:

(a) File Name: photo\_2019-03-31\_14-23-40.jpg

Created Date/Time: 7/14/2019 6:43:16 PM

MD5 Hash: fff46dba47d92a222e304c1d631671ad

This image showed the torso of a prepubescent white male being anally penetrated by an adult male's penis. The prepubescent male had a draw-string tied around his testicles causing them to swell and turn purple.

(b) File Name: cp gay hombre amarra a ni\_o.mp4

Modified Date/Time: 11/16/2018 8:05:16 AM(UTC-6)

MD5 Hash: 69e5556f19bad34460d7136d6cd609db



This video is approximately 00:52 (mm:ss) seconds in length and depicts a prepubescent white male between the age of eight (8) to ten (10) years old lying completely nude on a bed. The prepubescent male was blind-folded and his hands were tied to a post at the head of the bed. An adult white male lifted and tied the minor's legs up to the same post that his hands were tied to, causing the minors genitals and anus to be exposed to the camera. The adult male then performed oral sex on the minor male and masturbated for the duration of the video.

(c) File Name: video\_2019-04-28\_23-54-37.mp4

Modified Date/Time: 4/28/2019 6:54:50 PM(UTC-5)

MD5 Hash: ef987f4cd6af83e7cdb045464fdf72ce

This video is approximately 00:09 (mm:ss) seconds in length and depicts a prepubescent white male between the age of eight (8) to ten (10) years old performing oral sex on an adult white male.

14. During the investigation, Detective Helms was able to verify LAWSON'S home address, located at 1299 Electric Avenue, Apartment E-206, Springdale, Arkansas 72764. On October 04, 2019, Detective Helms obtained a state search warrant for LAWSON'S residence and the warrant was signed by Washington County Circuit Court Judge, John Threet. On October 04, 2019 at approximately 12:30 hours, Springdale Detectives along with Homeland Security Investigations (HSI), Special Agents and Computer Forensic Analysts assigned to the Internet Crimes Against Children Task Force executed the state search warrant at LAWSON'S residence. HSI Computer Forensic Analysts conducted on-scene previews of electronic devices found inside of LAWSON'S apartment and more evidence of child pornography images and videos were found saved on computer devices owned by LAWSON. Detective Helms

subsequently seized four (4) laptop computers, one (1) Apple iPad tablet and two additional cellular phones. The phones are described as an Alcatel TCL, model LX, and a Microsoft Lumina, model RM-1073. The State search warrant allowed for on-scene and off-scene computer forensic processing; therefore, these devices were analyzed at a later date by Computer Forensic Analysts assigned to the HSI, Fayetteville office.

15. The forensic examination of a Lenovo laptop computer (S/N: CB32278140) revealed seven different file folders saved to the desktop screen and each file contained child abuse material. Several email accounts of interest were also identified in the forensic processing and each email address was found to be used in various chatting programs where LAWSON was observed sharing child pornography images and videos with other users. The email addresses were identified as [cocksuckerwithagun@gmail.com](mailto:cocksuckerwithagun@gmail.com), [pervyfwb@gmail.com](mailto:pervyfwb@gmail.com), [madwirelesspllc@gmail.com](mailto:madwirelesspllc@gmail.com), [pervyfwb69@icloud.com](mailto:pervyfwb69@icloud.com), [fwb69@icloud.com](mailto:fwb69@icloud.com), [leatherneck4life@icloud.com](mailto:leatherneck4life@icloud.com), and [mattielawson@me.com](mailto:mattielawson@me.com).

16. The email addresses [cocksuckerwithagun@gmail.com](mailto:cocksuckerwithagun@gmail.com) and [fwb69@icloud.com](mailto:fwb69@icloud.com) were linked to a video chat application called ringcentral.com. The email addresses [cocksuckerwithagun@gmail.com](mailto:cocksuckerwithagun@gmail.com) and [pervyfwb@gmail.com](mailto:pervyfwb@gmail.com) were found connected to another video chat application called zoom.us. Several videos from ringcentral.com and zoom.us were found on the device. Based on artifacts located on the computer, it appears that LAWSON, was using various video chat applications such as Zoom, Ring Chat, Telegram, and Mega to communicate with other users and share child pornography. The screen recorded chat videos depicting users sharing child abuse material openly in the chat rooms, while other chat room members masturbate and smoke or inject suspected methamphetamine. Recordings of these



videos and text documents containing chat logs were found saved in several places on the laptop computer. In the videos, LAWSON is visually identifiable and appears to be using pseudonyms, but the email addresses associated with the chat applications are identical to the ones listed in the user's Google Chrome settings which were recovered in the forensic processing.

17. During chat sessions, LAWSON made several statements regarding the children pictured in the photographs and videos that he shared with other members in the chat room. LAWSON indicated that he was the father of two children and commented that he was the person sexually assaulting them. Forensic investigators were able to identify exif data in a sexually explicit video which indicated the video was created on May 29, 2018 in Muldrow, Oklahoma. This sexually explicit video depicts a white male with tattoos matching LAWSON, masturbating a white male child between the ages of six to ten years old. The adult male also masturbates himself in front of the child.

18. Other recovered forensic artifacts revealed that LAWSON was using Apple devices. An Apple iPad belonging to LAWSON was recovered by Detective Helms on October 04, 2019, pursuant to a search warrant, at 1299 Electric Avenue, Apartment E-206, Springdale, Arkansas 72764. Due to the fact that LAWSON used iCloud accounts such as [pervyfwb69@icloud.com](mailto:pervyfwb69@icloud.com), [fwb69@icloud.com](mailto:fwb69@icloud.com), and [leatherneck4life@icloud.com](mailto:leatherneck4life@icloud.com), a search warrant is requested for these accounts. The other email addresses from non-Apple providers will also be requested from Apple due to the fact that they can be used as secondary authentication email addresses and may be connected to other iCloud accounts not yet known to this investigation.

19. Based on my knowledge and experience, I know that Cloud Service Providers have a tremendous amount of storage capacity, and this storage is distributed across physical storage media (i.e., hard drives) in multiple datacenters in multiple geographic locations. I also know that software keeps track of how data is stored in this environment, and that it has the ability to identify the physical location of any piece of data and reconstruct the pieces into their original format. I know from training and experience that individuals engaged in child pornography generally prefer to store images of child pornography in electronic form as computer files. The computer's ability to store images in digital form makes a computer an ideal repository for pornography. Even a small portable disk or computer hard drive can contain many child pornographic images. The images can be easily sent to or received from other computer users over the Internet. Further, both individual files of child pornography and the disks that contain the files can be mislabeled or hidden to evade detection. In my training and experience, individuals who view child pornography typically maintain their collections for many years and keep and collect items containing child pornography over long periods of time; in fact, they rarely, if ever, dispose of their sexually explicit materials. Based on the information discovered within the Lenovo laptop computer, LAWSON was using cloud-based storage providers such as Dropbox, Apple and Google. It is believed that LAWSON used these cloud-based storage providers for saving images and videos of child abuse material.



**BACKGROUND REGARDING APPLE ID AND iCloud**<sup>1</sup>

20. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

- a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.
- b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.
- c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.
- d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For

---

<sup>1</sup> The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: “U.S. Law Enforcement Legal Process Guidelines,” available at <http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf>; “Create and start using an Apple ID,” available at <https://support.apple.com/en-us/HT203993>; “iCloud,” available at <http://www.apple.com/icloud/>; “iCloud: iCloud storage and backup overview,” available at <https://support.apple.com/kb/PH12519>; and “iOS Security,” available at [http://images.apple.com/privacy/docs/iOS\\_Security\\_Guide.pdf](http://images.apple.com/privacy/docs/iOS_Security_Guide.pdf).

example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user's Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.



21. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

22. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.

23. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

24. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

25. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

26. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email



(iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud.

27. The stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

28. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the

account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

29. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

30. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

31. Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

#### **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**


32. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in



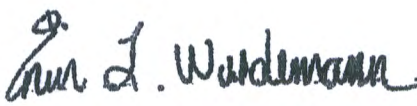
Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

### **CONCLUSION**

33. Therefore, your affiant respectfully requests this Court to issue a search warrant authorizing the search of Apple iCloud accounts, cocksuckerwithagun@gmail.com, pervyfwb@gmail.com, madwirelesspllc@gmail.com, fwb69@icloud.com, pervyfwb69@icloud.com, leatherneck4life@icloud.com, mattielawson@me.com, as well as any and all account information associated with Matthew LAWSON which is controlled and maintained by Apple Inc., as described in Attachment A, to seize the evidence, fruits, and instrumentalities described in Attachment B, which individually or collectively constitute violation(s) of **Title 18, United States Code, Sections 2251 (Production of Child Pornography), 2252A(a)(5)(B) and (b)(2) (Possession of Child Pornography), and 2252A(a)(1) and (b)(1) (Transportation of Child Pornography).**

  
Thomas Wooten, Task Force Officer  
Homeland Security Investigations

Affidavit subscribed and sworn to before me this 4<sup>th</sup> day of June 2020.

  
Honorable Erin L. Wiedemann  
United States Magistrate Judge



**ATTACHMENT A**

**PROPERTY TO BE SEARCHED**

This search warrant applies to all content and information associated with user ID(s) or email address: cocksuckerwithagun@gmail.com, pervyfwb@gmail.com, madwirelesspllc@gmail.com, fwb69@icloud.com, pervyfwb69@icloud.com, leatherneck4life@icloud.com, and mattielawson@me.com, as related to Matthew Roy LAWSON; and/or iTunes account information related to Matthew Roy LAWSON, that is stored at premises controlled by Apple, Inc., a company that accepts service of legal process; located at 1 Infinite Loop, M/S 36-SU, Cupertino, CA 95104, **from January 01, 2015 until present.**

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Apple**

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to any request made under Title 18, United States Code, Section 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

- a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);
- b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber



Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”);

c. Any and all image or videos associated with the account, including stored or preserved or previously deleted images still accessible by Apple, any and all Meta-data or embedded data associated with the images/videos; any and all information associated with the posting IP address and/or the geolocation and identification of any devices used to save or upload images;

d. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

e. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

f. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

g. All records pertaining to the types of service used; and

h. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken.



## **II. Information to be seized by the government**

All information described above in Section I, including correspondence, records, documents, photographs, videos, applications, communications, and electronic messages that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 2251, 2252, and 2252A including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);
- b. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;
- c. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);
- d. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and
- e. Evidence that may identify any co-conspirators or aiders and abettors for the above-listed crimes, including records that help reveal their whereabouts.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC  
RECORDS PURSUANT TO FEDERAL RULES OF  
EVIDENCE 902(11) AND 902(13)**

I, \_\_\_\_\_, attest, under penalties of perjury by the laws of the United States of America pursuant to Title 28, United States Code, Section 1746, that the information contained in this certification is true and correct. I am employed by Apple Inc., and my title is \_\_\_\_\_. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Apple Inc. The attached records consist of \_\_\_\_\_  
\_\_\_\_\_ (pages/CDs/megabytes).

I further state that:

a. All records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of **Apple Inc.**, and they were made by Apple Inc., as a regular practice; and

b. Such records were generated by Apple Inc., electronic process or system that produces an accurate result, to wit:

1. The records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Apple Inc., in a manner to ensure that they are true duplicates of the original records; and

2. The process or system is regularly verified by Apple Inc., and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature